US009219609B2

(12) **United States Patent**
Hird et al.

(10) **Patent No.:** **US 9,219,609 B2**
(45) **Date of Patent:** ***Dec. 22, 2015**

(54) **METHOD AND SYSTEM FOR MULTIPLE PASSCODE GENERATION**

(71) Applicant: **CA, Inc.**, Islandia, NY (US)

(72) Inventors: **Geoffrey Hird**, Cupertino, CA (US); **Rammohan Varadarajan**, Cupertino, CA (US); **James D. Reno**, Scotts Valley, CA (US)

(73) Assignee: **CA, Inc.**, New York, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/072,392**

(22) Filed: **Nov. 5, 2013**

(65) **Prior Publication Data**

US 2014/0068271 A1 Mar. 6, 2014

Related U.S. Application Data

(63) Continuation of application No. 13/020,867, filed on Feb. 4, 2011, now Pat. No. 8,613,065.

(60) Provisional application No. 61/304,572, filed on Feb. 15, 2010.

(51) **Int. Cl.**

G06F 21/00	(2013.01)
H04L 9/32	(2006.01)
G06F 21/31	(2013.01)
H04L 29/06	(2006.01)
H04L 9/08	(2006.01)
H04L 9/16	(2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/3226*** (2013.01); ***G06F 21/31*** (2013.01); ***H04L 9/0877*** (2013.01); ***H04L 9/16*** (2013.01); ***H04L 63/0838*** (2013.01)

(58) **Field of Classification Search**
CPC ... G06F 21/31; H04L 63/0838; H04L 9/0877; H04L 9/16; H04L 9/3326
USPC 713/184
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2006/0107312 A1*	5/2006	Fiske	726/5
2008/0168543 A1*	7/2008	von Krogh	726/6

(Continued)

OTHER PUBLICATIONS

Viorel, Passcode Based Authentication Protocol, 2010, IEEE, pp. 204-210.*

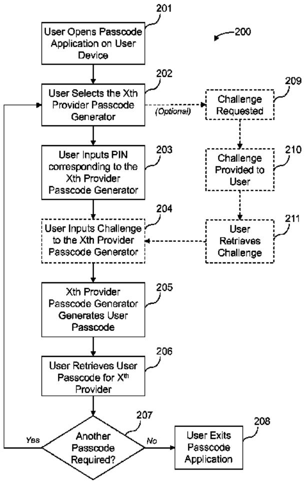
(Continued)

Primary Examiner — Christopher Brown
Assistant Examiner — Jenise Jackson
(74) *Attorney, Agent, or Firm* — Vierra Magen Marcus LLP

(57) **ABSTRACT**

This invention relates to a method and a system for generating user passcodes for each of a plurality of transaction providers from a mobile user device. A method and system for activating a plurality of passcode generators on a user device configured with a passcode application installed on the user device is provided. Each of the passcode generators may correspond to a different user account or transaction provider, such that each passcode generator provides a user passcode configured for the corresponding account or transaction provider. One or more of the passcode generators may include a passcode generating algorithm and a passcode key. Access to one or more of the passcode generators may require providing a PIN or a challenge.

19 Claims, 2 Drawing Sheets


200
201
User Opens Passcode Application on User Device
202
User Selects the Xth Provider Passcode Generator
(Optional)
209
Challenge Requested
210
Challenge Provided to User
211
User Retrieves Challenge
203
User Inputs PIN corresponding to the Xth Provider Passcode Generator
204
User Inputs Challenge to the Xth Provider Passcode Generator
205
Xth Provider Passcode Generator Generates User Passcode
206
User Retrieves User Passcode for Xth Provider
207
Another Passcode Required?
Yes
No
208
User Exits Passcode Application

(56) References Cited

U.S. PATENT DOCUMENTS

2009/0119761	A1 *	5/2009	Dharmarajan	726/6
2009/0214028	A1 *	8/2009	Schneider	380/44
2009/0328165	A1 *	12/2009	Cook et al.	726/6
2011/0113237	A1 *	5/2011	Hird	G06F 21/34 713/155
2011/0197266	A1 *	8/2011	Chu et al.	726/5
2012/0030759	A1 *	2/2012	Goldman	G06F 21/56 726/23

OTHER PUBLICATIONS

Tian et al, Privacy Preserving Personalized Access Control Service at Third Service Provider, 2011, IEEE, pp. 694-695.*

* cited by examiner

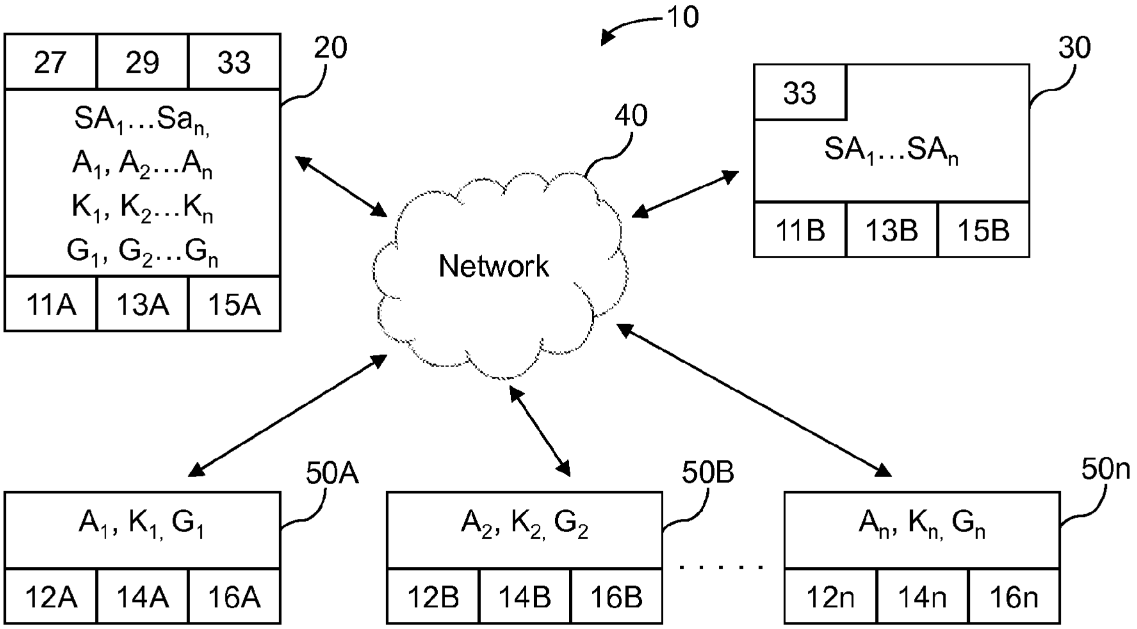

10
27
29
33
20
SA1...San,
A1, A2...An
K1, K2...Kn
G1, G2...Gn
11A
13A
15A
40
Network
33
30
SA1...SAn
11B
13B
15B
50A
A1, K1, G1
12A
14A
16A
50B
A2, K2, G2
12B
14B
16B
50n
An, Kn, Gn
12n
14n
16n

FIG. 1

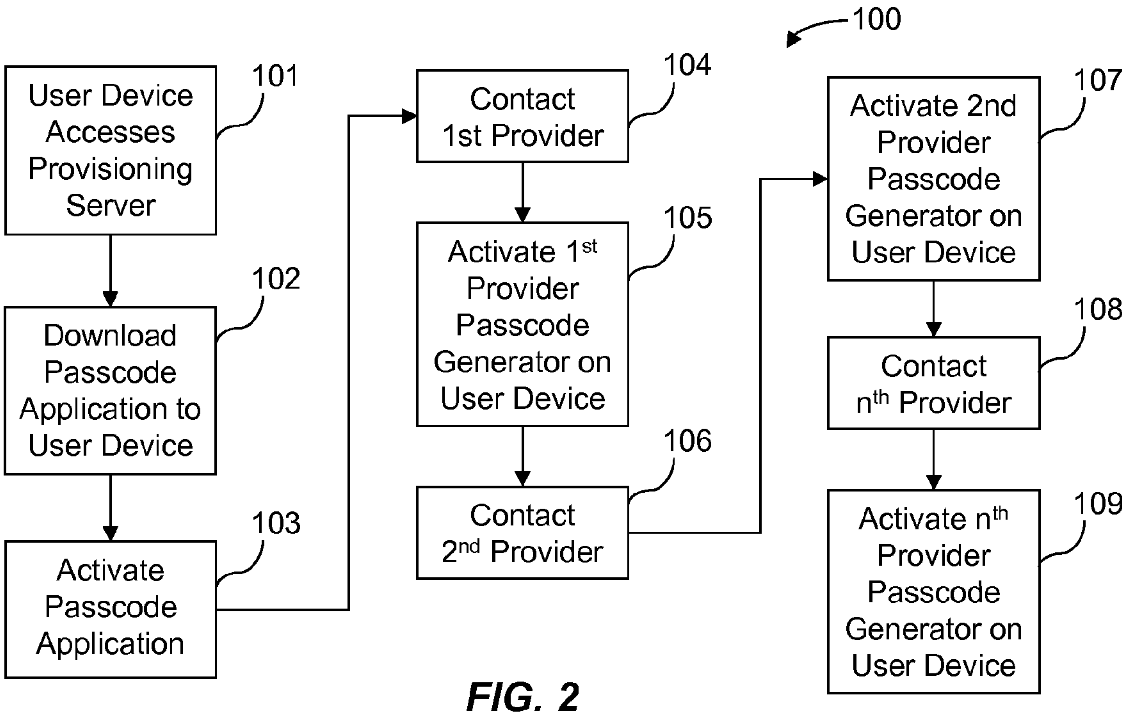

100
User Device Accesses Provisioning Server
101
Download Passcode Application to User Device
102
Activate Passcode Application
103
Contact 1st Provider
104
Activate 1st Provider Passcode Generator on User Device
105
Contact 2nd Provider
106
Activate 2nd Provider Passcode Generator on User Device
107
Contact nth Provider
108
Activate nth Provider Passcode Generator on User Device
109

FIG. 2

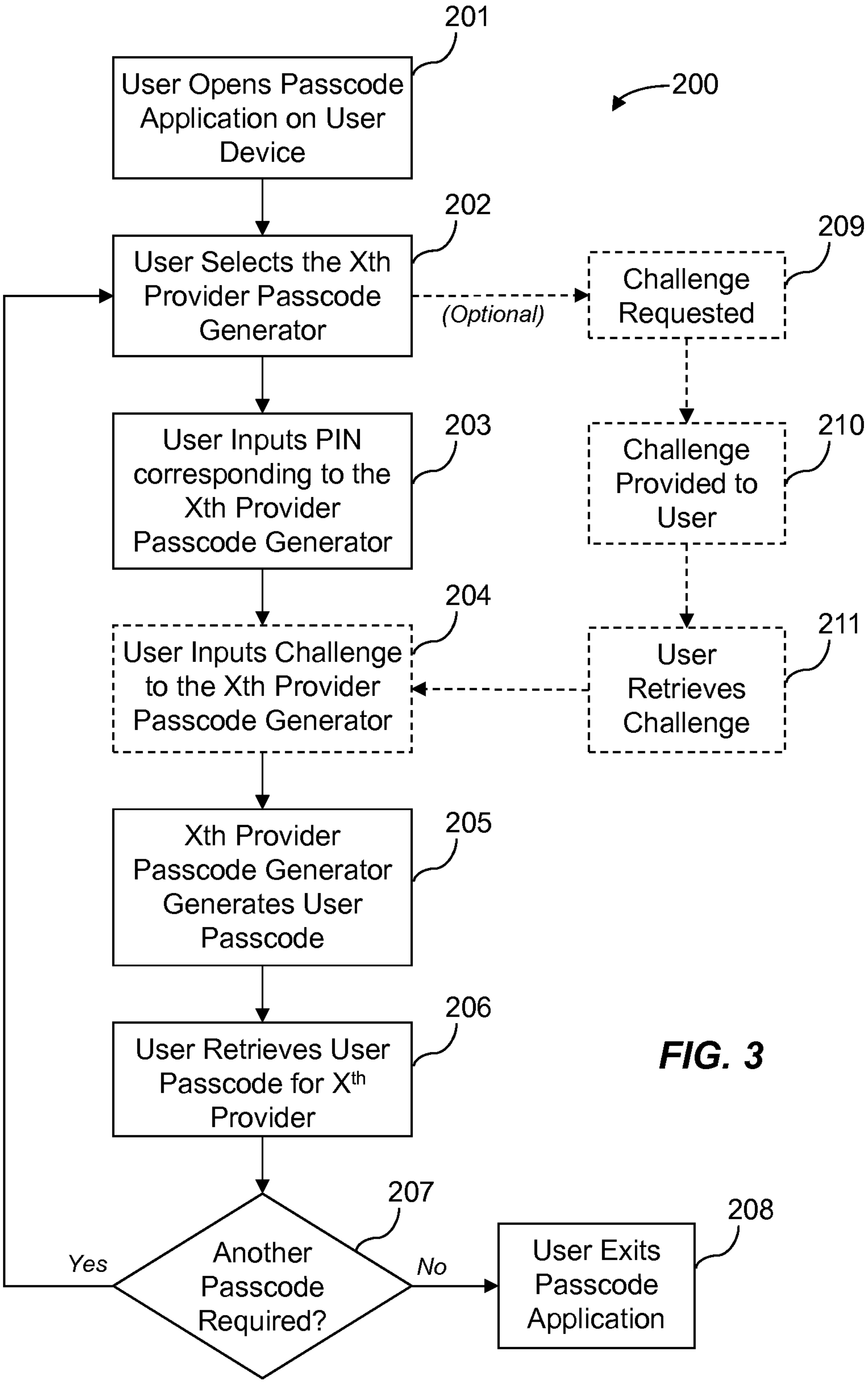

201
User Opens Passcode Application on User Device
200
202
User Selects the Xth Provider Passcode Generator
(Optional)
209
Challenge Requested
203
User Inputs PIN corresponding to the Xth Provider Passcode Generator
210
Challenge Provided to User
204
User Inputs Challenge to the Xth Provider Passcode Generator
211
User Retrieves Challenge
205
Xth Provider Passcode Generator Generates User Passcode
206
User Retrieves User Passcode for Xth Provider
207
Another Passcode Required?
Yes
No
208
User Exits Passcode Application

FIG. 3

METHOD AND SYSTEM FOR MULTIPLE PASSCODE GENERATION

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of and claims the benefit of U.S. patent application Ser. No. 13/020,867 filed on Feb. 4, 2011, published as US 2011/0202984 on Aug. 18, 2011 and issued as U.S. Pat. No. 8,613,065 on Dec. 17, 2013, which claims the benefit of U.S. Provisional Patent Application No. 61/304,572 filed on Feb. 15, 2010, which are hereby incorporated by reference in their entirety.

TECHNICAL FIELD

This invention relates to a method and a system for generating user passcodes for each of a plurality of transaction providers from a mobile user device.

BACKGROUND

Many methods exist for providing a dynamic passcode value, which is often referred to as a one time passcode (OTP), including OTP keyfobs and Universal Serial Buses (USBs), smart cards and various software solutions. Each keyfob, smartcard, etc., is typically dedicated to a single user account from a single provider. A user with multiple accounts from one or more providers or institutions may be required to obtain, possess, and use a separate keyfob or passcode generating device for each account. This presents an inconvenience for the user, requiring the user to carry and maintain multiple pieces of hardware to obtain user passcodes corresponding to each of a plurality of user accounts.

SUMMARY

The ability to conveniently obtain user passcodes from a single user device for each of a number of accounts or transaction providers, where the user device is preferably a mobile device such as a mobile phone or a personal digital assistant (PDA), presents numerous advantages to the user. User convenience is enhanced by having to possess and access only one device to obtain passcodes for any of a plurality of accounts with any of a plurality of transaction providers. Security of the passcode generators is enhanced due to consolidation of a number of passcode generators on a single device, e.g., the user's mobile phone or PDA, which is typically kept on or close to the user's person and which is frequently monitored by the user. The probability that the user's mobile device and passcode generators provided thereon may be misplaced, lost, or stolen is reduced in comparison with the probability of misplacement or loss of an individual keyfob, USB, smart card, or other passcode generating device, which may be intermittently used, set aside or stored in various locations apart from the user. Convenience is further enhanced due to the mobility of the single passcode generating device, and accessibility from any location or at any time the user requires a passcode to complete a transaction.

Accordingly, a system and method are provided for activating a plurality of passcode generators on a user device via a passcode application installed on the user device. The user device may be, for example, a mobile phone or PDA. Each of the passcode generators on the user device may correspond to a different user account or transaction provider, such that each passcode generator provides a user passcode configured for the corresponding account or transaction provider.

The method may include installing a passcode application on the user device and activating a plurality of passcode generators on the user device using the passcode application. Each of the plurality of provider passcode generators is configurable to provide a user passcode for a transaction between a user and the corresponding provider associated with the passcode generator. The method may further include accessing one or more provider interfaces via the user device and/or passcode application to receive information configured to activate a passcode generator corresponding to the provider on the user device. Installing the passcode application on the user device may include installing one or more algorithms which may be configured to generate passcodes. Further, a provider passcode key may be obtained by the passcode application and used to configure and/or activate a corresponding provider passcode generator on the user device. A PIN and/or challenge may be required to access the passcode application and/or one or more of the provider passcode generators.

The system may include a passcode application. But passcode application may be used to configure and/or to activate a plurality of passcode generators on a user device. The user device may be configured to receive the passcode application. A provisioning server may be configured to provide the passcode application to the user device, and a plurality of provider interfaces each configurable to provide passcode information related to the corresponding provider. Each of the plurality of provider passcode generators may be configured for activation on the user device to communicate with a corresponding provider server, to obtain passcode information to activate each provider passcode generator on the user device such that the user can obtain a provider passcode configured as a user passcode for the corresponding provider. The system may include one or more algorithms, wherein each of the algorithms may be configured to generate at least one provider passcode. The system may further include one or more keys, wherein each of the keys may be configured to generate a respective provider passcode which corresponds to the user's account with that respective provider. The system may generate a PIN and/or challenge for input to access the passcode application and/or to access one or more of the provider passcode generators.

The above features and advantages and other features and advantages of the present invention are readily apparent from the following detailed description of the best modes for carrying out the invention when taken in connection with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a schematic illustration of a user device-based system for generating a user passcode for each of a plurality of providers;

FIG. **2** is a graphical flow chart describing a method for activating a plurality of passcode generators on a user device; and

FIG. **3** is a graphical flow chart describing a method for obtaining a passcode from one of a plurality of passcode generators on a user device.

DETAILED DESCRIPTION

Referring to the drawings, wherein like reference numbers correspond to like or similar components throughout the several figures, there is shown in FIG. **1** a schematic illustration of a system **10** for generating a user passcode for each of a plurality of providers on a user device. The system **10** includes a user device **20**, which may be any of a variety of user mobile phones, personal digital assistances (PDAs) and handheld devices (iPhone™, Blackberry™, etc.). The system **10** includes a provisioning server **30**, and a plurality of provider servers **50**A, **50**B . . . **50***n*, which are each configured to communicate with and/or through a network **40**, which may be, for example, the internet.

The user device **20** is configured to communicate with the network **40** through an interface **15**A, which may be a modem, mobile browser, wireless internet browser or similar means. The user device **20** further includes a memory **13**A, a central processing unit (CPU) **11**A and one or more algorithms which may be one or more standard algorithms (SA_n) or other algorithms (A_n) adaptable as passcode-generating algorithms. Memory **13**A can include, by way of example, Read Only Memory (ROM), Random Access Memory (RAM), electrically-erasable programmable read only memory (EEPROM), etc., of a size and speed sufficient for executing one or more algorithms $SA_1 \ldots SA_n, A_1, A_2 \ldots A_n$ and/or one or more passcode generators $G_1, G_2 \ldots G_n$ activated on the user device **20**. The user device **20** further includes a display **29** configurable to display a passcode application, a passcode menu, passcodes and/or challenges. The user device **20** includes an input **27** configured to receive input from the user, e.g., a keypad through which the user may key in a PIN and/or a challenge, a camera configured to receive a retinal scan, a fingerprint pad, an electronic receiver, or a combination of these. A passcode application **33**, which may include one or more standard algorithms $SA_1 \ldots SA_n$ and/or other software, may be provided and installed on the user device **20** from the provisioning server **30**, through the network **40**.

The provisioning server **30** is adapted to communicate with the network **40** through an interface **15**B, which may be a modem, website or similar means. The provisioning server **30** further includes a memory **13**B, a CPU **11**B, one or more algorithms which may be one or more standard algorithms (SA_n) or other algorithms (A_n) adaptable as passcode generating algorithms, and a passcode application **33**. The memory **13**B can include, by way of example, ROM, RAM, EEPROM, etc., of a size and speed sufficient for configuring, providing and activating the passcode application **33** on the user device **20**, through the network **40**.

Still referring to FIG. **1**, the system **10** further includes a first provider server **50**A, which corresponds to a first provider and which may be configured to communicate with the network **40** through a first provider interface **16**A e.g., a first provider website. The first provider server **50**A includes a memory **14**A and a CPU **12**A. the first provider server **50**A may be configured to provide a first provider algorithm A_1 and/or a first passcode key K_1, where the algorithm A_1 and/or the passcode key K_1 may be configured to provide a first passcode generator G_1. The algorithm A_1, the passcode key K_1, and/or the passcode generator G_1 may be configured to generate a user passcode configured for use with the first provider. Memory **14**A can include, by way of example, ROM, RAM, EEPROM, etc., of a size and speed sufficient for configuring, providing and/or activating an algorithm A_1, a passcode key K_1 and/or a passcode generator G_1 on the user device **20**, through the network **40** and/or the passcode application **33**.

System **10** further includes at least a second provider server **50**B corresponding to a second provider. The provider server **50**B may be configured similarly to the provider server **50**A, e.g., the second provider server **50**B may be configured to communicate with a network **40** through a second provider interface **16**B which may be, for example, a website of the second provider. The second provider server **50**B includes a memory **14**B and a CPU **12**B and may be configured to provide a second provider algorithm A_2 and/or a passcode key K_2. The algorithm A_2 and/or the passcode key K_2 may be configured to provide a second passcode generator G_2. The algorithm A_2, the passcode key K_2, and/or the second passcode generator G_2 may be configured to generate a user passcode configured for use with the second provider. The memory **14**B can include, by way of example, ROM, RAM, EEPROM, etc., of a size and speed sufficient for configuring, providing and/or activating an algorithm A_2, passcode key K_2 and/or passcode generator G_2 on the user device **20**, through the network **40** and/or phone passcode application **33**.

System **10** may include a plurality of additional provider servers generally indicated as **50***n*, and corresponding to a plurality of additional providers, wherein the nth server **50***n* corresponds to an nth provider. As discussed previously, the server **50***n* may be configured similarly to the provider server **50**A, e.g., the nth provider server **50***n* may be configured to communicate with the network **40** through a nth provider interface **16***n* which may be, for example, a website of the nth provider. The nth provider server **50***n* includes a memory **14***n* and a CPU **12***n* and may be configured to provide a second provider algorithm A_n and/or a passcode key K_n, where the algorithm A_n and/or the passcode key K_n may be configured to provide a passcode generator G_n. The algorithm A_n, the passcode key K_n, and/or the nth passcode generator G_n may be configured to generate a user passcode configured for use with the nth provider. The memory **14***n* can include, by way of example, Read Only Memory (ROM), Random Access Memory (RAM) electrically-erasable programmable read only memory (EEPROM), etc., of a size and speed sufficient for configuring, providing and/or activating an algorithm A_n, a passcode key K_n and/or a passcode generator G_n on the user device **20**, through the network **40** and/or the passcode application **33**.

Referring now to FIGS. **2** and **3**, a method for providing a plurality of passcode generators $G_1 \ldots G_n$ on a user device **20** is provided, which may include installing a passcode application **33** on the user device **20** and activating the plurality of passcode generators $G_1 \ldots G_n$ on the user device **20** via the passcode application **33**, wherein each of the plurality of passcode generators $G_1 \ldots G_n$ is configurable to provide a user passcode for a transaction between the user and the provider corresponding to the provider passcode generator $G_1 \ldots G_n$ on the user device **20**.

Shown in FIG. **2** and indicated generally at **100**, is a graphical flow chart describing one possible method for activating a plurality of passcode generators on a user device **20**. Referring to FIG. **2**, referencing the system **10** of FIG. **1**, and beginning with step **101**, a user, through a user device **20**, accesses a provisioning server **30** to download, at step **102**, a passcode application **33** to the user device **20**. The user may be required to provide a user name, user device information or other identifying and authenticating information as needed to activate, at step **103**, the passcode application **33** on the user device **20**. The provisioning system **30** may provide the user an activation code, which the user may be required to input at step **103** to activate the passcode application **33** installed on the user device **20**. The passcode application **33** may include one or more standard algorithms $SA_1 \ldots SA_n$ which may be adaptable to generate passcodes using a key $K_1 \ldots K_n$ configured by a provider and provided to the user device **20**. Standard algorithms $SA_1 \ldots SA_n$ may be, by way of example and not intended to be limiting in scope, one or more algorithms adopted and/or approved by the Initiative for Open Authentication (OATH), such as a hash-based message authentication code (HMAC) one time password (HOTP) algorithm, a time-based one time password (TOTP) algorithm, a one time password challenge/response algorithm (OCRA) or other OATH-approved algorithm.

Continuing with step **104** of FIG. **2**, the user contacts the first provider **50**A through, for example, a first provider interface **16**A (referring for FIG. **1**), using the user device **20** and the passcode application **33**. The user provides information to the first provider **50**A as required to activate a first provider passcode generator G_1 on the user device **20**. For example, the user may be required to provide to the first provider system **50**A the user's account number for the first provider, user device information, such as the type or model of the user device, user contact information which may include a phone number or email address, to install or configure a first provider passcode generator G_1 via the passcode application **33** on the user device **20**, and/or an access code previously communicated by first provider system **50**A to the user.

At step **105** of FIG. **2**, the first passcode generator G_1 is downloaded to the user device **20** and the passcode application **33**. The user provides, if required, additional input to activate the first passcode generator G_1 on the user device **20**. For example, the user may be required to input an activation code to complete step **105**. The user may additionally be required to input a PIN either provided by the first provider or established by the user during the activation session with the first provider, to access the first provider passcode generator G_1on the user device **20**.

The first provider passcode generator G_1 is configured to generate, on the user device **20**, passcodes retrievable by the user for use in transactions with the first provider. The first passcode generator G_1 may be configured by the first provider system **50**A and installed to the passcode application **33** on the user device **20**. Alternatively, a first algorithm A_1 may be installed to the passcode application **33**, which may be a non-standard algorithm A_1 which is proprietary to the first provider, or the first provider may select an algorithm from the standard algorithms $SA_1 \ldots SA_n$ included in the passcode application **33** to configure a first passcode generator G_1 on user device **20**. The first provider system **50**A may provide a first key K_1 which is uniquely configured for the user's first provider account. The first key K_1 may be adaptable for use with an algorithm A_1 to configure the first passcode generator G_1. As discussed previously, the algorithm A_1 may be a standard algorithm provided by the passcode application **33** or may be a proprietary or non-standard algorithm provided by the first provider system **50**A. The first key K_1 may be, for example, a symmetric key, a non-symmetric key, a data encryption standard (DES) key, an advanced encryption standard (AES) key, a secret, a secret byte array, a card verification key (CVK), a unique derivation key (UDK), a unique DEA key A (UDKA), a unique DEA key B (UDKB), a seed or an indexed key list. Additionally, the first key K_1 may be encrypted, obfuscated, cryptographically camouflaged or otherwise secured by the first provider system **50**A and/or the passcode application **33** prior to being used to configure the first passcode generator G_1.

After the first passcode generator G_1 is installed and activated on the user device **20**, the user may continue at step **106** to contact a second provider system **50**B, again using the passcode application **33** and the user device **20**, to install and activate at step **107** a second passcode generator G_2 corresponding to a different user account, e.g., a user account with the second provider, using a method as discussed previously for the first provider and the first passcode generator. Similarly, after the second passcode generator G_2 is installed and activated on the user device **20**, the user may continue at step **108** to contact a third provider system, again using the passcode application **33** and the user device **20**, to install and activate at step **109** a third passcode generator corresponding to a different user account, e.g., a user account with the third provider, using a method as discussed previously for the first provider and first passcode generator. Steps **108** and **109** may be repeated to contact nth provider systems **50***n* and to activate nth passcode generators G_n using the passcode application **33** on the user device **20**.

Each of the algorithms $SA_1 \ldots SA_n$ may be any standard algorithm which may be configured or used for passcode generation, including any OATH-approved algorithm such as a HOTP algorithm, a TOTP algorithm, an OCRA algorithm or other OATH-approved algorithm. Each of algorithms $A_1 \ldots A_n$ may be a standard algorithm $SA_1 \ldots SA_n$ or may be another algorithm which may be proprietary to one or more of the provider systems **50**A . . . **50***n*. Each of the keys $K_1 \ldots K_n$ may be, for example, a symmetric key, a non-symmetric key, a DES key, an AES key, a secret, a secret byte array, a CVK, a UDKA, a UDKB, a seed or an indexed key list. Additionally, each of the keys $K_1 \ldots K_n$ may be encrypted, obfuscated, cryptographically camouflaged or otherwise secured by its respective provider system **50**A . . . **50***n* and/or the passcode application **33** prior to provided to the user device **20** and/or adapted to produce a respective passcode generator $G_1 \ldots G_n$.

For illustrative example and not intended to be limiting in scope, referring again to FIGS. **1** and **2**, a first provider **50**A may be a banking institution providing a passcode generator G_1 to a user for the user's ATM account. The first passcode generator G_1 may be configured with an algorithm A_1, which may be proprietary or unique to the banking institution, and a key K_1 which is unique to the user's ATM account, such that the first passcode generator G_1 is configured to generate a one-time PIN or passcode (OTP) on the user device **20**. The OTP generated on the user device **20** may be provided as a single use PIN for an ATM transaction corresponding to the user's ATM account and verifiable as the user's PIN by the banking institution **50**A. Continuing, for example, a second provider **50**B may be the user's employer providing a passcode generator G_2 to the user device **20** corresponding to the user's account on the employer's network or VPN. The second passcode generator G_2 may be configured with a standard TOTP algorithm, SA_1, and the second passcode generator G_2 may be configured to generate a dynamic user passcode at a set time increment, for example, every 60 seconds, on the user device **20**. The user may enter the generated dynamic user passcode with a user ID and/or PIN to gain access to the employer VPN. A third passcode generator G_3, for example, may be configured to generate a dynamic card verification value (CVV) for use as the CVV or security code associated with a credit card account, such as a Mastercard™ or Visa™ account. The third passcode generator G_3 may be configured within an algorithm, which may be a standard algorithm SA_2 or a proprietary algorithm A_2, and may be further configured with a key K_2 which is unique to the user's credit card account. The third passcode generator G_3 may be configured to generate a CVV which is usable for a predetermined number of transactions, for example, for a predetermined number of online purchases made with the user's corresponding Mastercard™ or Visa™. The nth passcode generator G_n, again by way of example, may be configured to generate a dynamic (one-time or temporary) authorization code which must be inputted online in conjunction with other authenticating information to authorize a secured transaction, for example, a sale of securities by a nth provider broker or release of medical information by a nth provider medical insurer. The collective first through nth passcode generators $G_1 \ldots G_n$ are installed and activated via the passcode application **33** on the user device **20**, providing the capability for the user, through the user device **20**, to conveniently generate and retrieve a plurality of dynamic passcode values each generated from a unique passcode generator and/or key and corresponding to a different provider account or system with which the user conducts transactions.

A passcode generator may be configured to provide more than one passcode corresponding to more than one provider, by activating more than one passcode key on the generator usable with that generator's passcode algorithm. For illustrative example, and not intending to be limiting in scope, a credit card passcode generator G_1 may be configured by the passcode application **33** with an algorithm SA_1 which can provide passcodes for a variety of credit cards, for example, Visa™ and Mastercard™ credit cards. The passcode application **33**, when activating a new provider account, would recognize whether the new provider account corresponds to the existing passcode generator G_1 and passcode algorithm SA_1, and, rather than configure a new passcode generator for the new provider, instead may configure the existing passcode generator G_1 for the new provider account. For example, a first passcode key K_1 may be activated on a credit card passcode generator G_1 corresponding to a user's first Visa™ account with a first provider **50**A. A second passcode key K_2 may be activated on the same credit card passcode generator G_1 corresponding to a user's Mastercard™ account, where the Mastercard™ provider uses the same passcode generating algorithm SA_1 as the first Visa™ provider **50**A. A third passcode key K_3 may be activated on the same credit card passcode generator G_1 corresponding to a user's second Visa™ account, where the second Visa™ provider **50**D (wherein provider **50**D is one of a plurality of additional provider servers generally indicated as **50***n*) uses the same passcode generating algorithm SA_1 as the first Visa™ provider **50**A. A fourth passcode key K_4 may be activated on the same credit card passcode generator G_1 corresponding to a user's retailer/merchant credit card, where the retailer/merchant credit card provider system **50**E (wherein provider **50**E is another of a plurality of additional provider servers generally indicated as **50***n*) uses the same passcode generating algorithm SA_1 as the Mastercard™ and first and second Visa™ provider systems **50**A, **50**C, **50**D, and so on. In this manner, further convenience is enjoyed by the user, who may select from multiple provider accounts within a single passcode generator G_1 to obtain a passcode for the selected account. Efficiency is gained by configuring multiple user accounts on the same account generator G_1, by reducing, for example, the memory required to store and operate multiple account passcode generators on a single user device.

Referring now to FIG. **3**, illustrated is a graphical flow chart describing a method generally indicated at **200** for obtaining a passcode from one or more of a plurality of passcode generators on the user device **20**. As shown in FIG. **3**, and referencing the system elements of FIG. **1**, a user at step **201** opens the passcode application **33** on the user device **20**, where the passcode application **33** has already been populated by a plurality of activated provider passcode generators $G_1 \ldots G_n$. Each of the provider passcode generators $G_1 \ldots G_n$ is configured to generate a passcode for the user which is recognizable by the provider corresponding to the passcode generator as a verifiable passcode from the user and corresponding to the user's provider account. As discussed previously, by way of example and not to be limiting in scope, a provider may be a banking institution providing a passcode usable as a PIN for an ATM transaction or online transaction; a secure network providing an passcode to authenticate the user for access to a VPN or other secure network; a credit/debit card issuer providing a passcode which may be used as a CVV for an online payment transaction, or a services provider such as a brokerage, a medical provider, or an insurance carrier providing a passcode for authorization of release of funds or confidential information. The user, at step **202**, accesses the passcode application **33** and selects the provider passcode generator corresponding to the provider for which the user requires a passcode. For example, the user may be conducting a transaction with a provider system **50**X corresponding to a provider X, wherein provider system **50**X is one of the plurality of additional provider systems generally indicated as **50***n*. As shown in FIG. **3**, the user selects the Xth provider passcode generator G_x, wherein G_x is one of the passcode generators $G_1 \ldots G_n$ selectable from a menu or other display **29** provided by the passcode application **33**. The passcode application **33** may provide a menu or other display as a listing of the provider names depicted in text or pictorially, for example, by displaying logos corresponding to each provider, or by any other means suitable to facilitate user convenience in selecting the desired provider passcode generator G_x at step **202**.

At step **203**, the user inputs a PIN corresponding to the Xth provider passcode generator G_x. The PIN may be in any configuration which can be input into user device **20**. By way of non-limiting example, the PIN may be a character string of one or more alpha-numeric or special characters inputted into the keypad, a picture or a graphic selected from the device screen, a challenge transmitted to the user's device as a short message service (SMS) message, text message or voice mail, a datum or an electronic signal transmitted from the user device **20**, a retinal scan provided to the user device's camera, or a fingerprint provided to a print pad on the user device **20**. The PIN input may be provided by the user device **20** automatically, for example, the PIN may be provided by passcode application **33**, or as a device identifier which is unique to or generated by the user's device **20**. This latter example provides additional security that the passcode application **33** and/or the passcode generator G_x has not been ported or copied over to another (unauthorized) device, by requiring a user device parameter or identifier that is unique to the user device **20** as the PIN. Alternatively, step **202** may be optional, e.g., a PIN input may not be required to generate a passcode. In this configuration, the process may proceed directly from user selection of the provider passcode generator G_x at step **202** to the passcode generation at step **205**, without further user input.

Following input of the user PIN corresponding to the passcode generator G_x at step **203**, the user may optionally be required to input a challenge at step **204**. The challenge, as previously discussed for the PIN, may be in any configuration which can be input into the user device **20**. For example, the challenge may be configured as a character string of one or more alpha-numeric or special characters, a picture or graphic, a datum or an electronic signal, a retinal scan or a fingerprint. At optional step **209**, a request for a challenge may be initiated by the passcode application **33** or by passcode generator G_x. The challenge is provided to the user at optional step **210**, by any suitable means, for example, as a SMS text message, email or voice mail. The challenge may be provided, for example, as a value, as an instruction requiring the user to input the purchase or payment amount of the transaction, or as a challenge question requiring the user to input an answer which may be known only by the user. The user retrieves the challenge at optional step **211** and at optional step **204** inputs the challenge value to the provider passcode generator G_x.

After the user has input the PIN at step **203**, and if required to do so, after the user has input a challenge to the passcode generator G_x at step **204**, the passcode generator G_x at step **205** generates a user passcode corresponding to the user's Xth provider account. The user retrieves the user passcode for use in a transaction with the Xth provider at step **206** by any suitable means. For example, if the passcode is provided to the display **29** of the user device **20** in human readable characters, the user may read the passcode from the display **29** to retrieve it for input into the Xth provider interface or another transaction interface in communication with the Xth provider system **50**X.

Referring now to step **207**, if the user requires another passcode for a subsequent transaction with a different provider, the user selects, at step **202**, the passcode generator corresponding with the different provider, and repeats steps **203** through **206** as required for that provider's passcode generator. Alternatively, at step **207**, if the user does not require any further passcodes at the present time, the user may exit the passcode application at step **208**.

Various optional configurations of the passcode application are possible. For example, the passcode application **33** may be further secured with a separate PIN, or may be secured by a locking mechanism(s) available on the user device **20**. The PIN for a first, second and nth passcode generator may be configured as the same PIN, e.g., having the same PIN value, for all passcode generators, increasing user convenience by decreasing the number of PIN values the user must memorize. One or more of the passcode generator keys $K_1 \ldots K_n$ may be cryptographically camouflaged such that the input of an invalid PIN may produce a passcode which is formatted for input into the provider interface, however the passcode generated in response to the invalid PIN will also be invalid, e.g., the invalid passcode provided will not be verifiable as a user passcode for the user's account if input into the provider interface.

The passcode application may configure a passcode generator on the user device, using a standard or recognized algorithm provided by the passcode application and a unique key generated by the provider and specific to the user account. The provider interface may send a proprietary (non-standards and/or unique) provider algorithm and a user account-specific key to the passcode application for the passcode application to configure as a passcode generator on the user device. Alternatively, the passcode application may receive the provider passcode generator directly from the provider, fully configured for the user's account.

Additional advantages, such as the ability to reset the passcode counter for a passcode generator through the user device may be provided, eliminating the inconvenience of contacting a provider in the event of passcode nonsynchrony. The various passcode generators provided by the passcode application may be updated automatically on the user device and without the need to replace the passcode generating hardware or the user's account card, as may be the instance if the passcode generator was configured as a provider dedicated keyfob or USB or, if the users card was configured as a passcode-generating smart card.

While the best modes for carrying out the invention have been described in detail, those familiar with the art to which this invention relates will recognize various alternative designs and embodiments for practicing the invention within the scope of the appended claims.

The invention claimed is:

1. A system comprising:

a user device comprising an interface, a memory, and a processing unit, wherein the user device is configured to receive a passcode application through the interface over a network from a provisioning server and to store the passcode application in the memory;

a first passcode generating algorithm recorded in the memory;

wherein the user device is configured to receive, over the network via the interface of the user device:

first passcode information from a first provider interface associated with a first provider;

second passcode information from a second provider interface associated with a second provider;

third passcode information from a third provider interface associated with a third provider;

a first passcode generator defined by the first provider interface; and

a second passcode generator defined by the second provider interface;

wherein the user device is configured to execute the passcode application on the processing unit to:

generate a first passcode configured as a user passcode for the first provider using the first passcode generator, the first passcode generating algorithm, and the first passcode information;

generate a second passcode configured as a user passcode for the second provider using the second passcode generator, a second passcode generating algorithm, and the second passcode information;

activate an account with the third provider, wherein the user device being configured to activate the account comprises the user device being configured to:

recognize whether a third passcode generator and a third passcode generating algorithm defined by the third provider interface correspond to either the first passcode generator and the first passcode generating algorithm or the second passcode generator and the second passcode generating algorithm, and configure the first passcode generator for generating a user passcode for the third provider using the third passcode information and the first passcode generating algorithm responsive to a determination that the third passcode generator and the third passcode generating algorithm correspond to the first passcode generator and the first passcode generating algorithm; and

generate a third passcode configured as the user passcode for the third provider using the first passcode generator, the first passcode generating algorithm, and the third passcode information.

2. The system of claim **1**, wherein the first passcode information comprises a first key defined by the first provider.

3. The system of claim **1**, wherein the second passcode information comprises a second key defined by the second provider.

4. The system of claim **1**, wherein the user device further comprises:

an input that is configured to receive an access PIN to access the passcode application.

5. The system of claim **1**, wherein the user device further comprises:

an input that is configured to receive a first PIN to obtain the first passcode; and

wherein the input is configured to receive a second PIN to obtain the second passcode.

6. The system of claim **1**, wherein the user device further comprises:

an input that is configured to receive a challenge configured for input as one of a first challenge to obtain the first passcode, and a second challenge to obtain the second passcode.

7. The system of claim **1**, wherein the user device is configured to execute the passcode application on the processing unit to:

install the first passcode generator on the user device; and install the second passcode generator on the user device.

8. A method comprising:

receiving, on a user device, a passcode application;

receiving on the user device a first passcode generator defined by a first provider;

receiving on the user device a second passcode generator defined by a second provider;

activating the first passcode generator to generate a first passcode configured as a user passcode for a transaction between a user and the first provider, wherein activating the first passcode generator comprises using a first algorithm on the user device;

activating the second passcode generator on the user device to generate a second passcode configured as a user passcode for a transaction between a user and the second provider, wherein activating the second passcode generator comprises using a second algorithm on the user device;

performing an activation process for an account between the user and a third provider, including recognizing whether a third passcode generator and a third algorithm defined by the third provider corresponds to either the first passcode generator and the first algorithm on the user device or to the second passcode generator and the second algorithm on the user device;

responsive to a determination that the third passcode generator and the third algorithm correspond to the first passcode generator and the first algorithm on the user device, configuring the first passcode generator on the user device to use the first algorithm for generating a third passcode for a transaction between the user and the third provider.

9. The method of claim **8**, further comprising:

displaying one of the first passcode, the second passcode, and the third passcode on a display of the user device.

10. The method of claim **8**, further comprising:

receiving first provider information from a first provider interface via the user device; and

wherein the first provider information comprises a first passcode key configured to activate the first passcode generator on the user device.

11. The method of claim **10**, further comprising:

receiving second provider information from a second provider interface via the user device; and

wherein the second provider information comprises a second passcode key configured to activate the second passcode generator on the user device.

12. The method of claim **8**, wherein activating the first passcode generator comprises activating a first passcode key on the user device, wherein of the first algorithm and the first passcode key together are configured to generate the first passcode.

13. The method of claim **8**, wherein activating the second passcode generator comprises activating a second passcode key on the user device, wherein the second algorithm and the second passcode key together are configured to generate the second passcode.

14. The method of claim **8**, wherein configuring the first passcode generator on the user device for generating a third passcode for a transaction between the user and the third provider comprises:

activating a third passcode key on the first passcode generator, wherein the first algorithm and the third passcode key together are configured to generate the third passcode.

15. The method of claim **8**, further comprising:

inputting a PIN into the user device, wherein the PIN is one of an access PIN to access the passcode application, a first PIN to obtain the first passcode, and a second PIN to obtain the second passcode.

16. The method of claim **15**, wherein two or more of the access PIN, the first PIN and the second PIN are the same PIN.

17. The method of claim **8**, further comprising:

generating the third passcode using the first passcode generator, the first algorithm, and passcode information from the third provider.

18. A tangible, non-transitory computer-readable medium having instructions stored thereon that when executed by a processor cause the processor to: receive on a user device a passcode application;

receive on the user device a first passcode generator defined by a first provider;

receive on the user device a second passcode generator defined by a second provider;

activate the first passcode generator using a first algorithm on the user device to generate a first passcode configured as a user passcode for a transaction between a user and the first provider;

activate the second passcode generator using a second algorithm on the user device to generate a second passcode configured as a user passcode for a transaction between a user and the second provider;

perform an activation process for an account between the user and a third provider, comprising causing the processor to recognize whether a third passcode generator and a third algorithm defined by the third provider corresponds to either the first passcode generator and the first algorithm on the user device or to the second passcode generator and the second algorithm on the user device;

responsive to a determination that the third passcode generator and the third algorithm correspond to the first passcode generator and the first algorithm on the user device, configure the first passcode generator on the user device for generating a third passcode for a transaction between the user and the third provider using the first algorithm.

19. The tangible, non-transitory computer-readable medium of claim **18**, wherein the instructions further cause the processor to:

receive passcode information from a provider interface associated with the third provider; and

generate the third passcode using the first passcode generator, the first algorithm, and the passcode information from the third provider.

* * * * *